УДК: 323.21

Дунаєва Л.М.,
доктор політичних наук,
професор кафедри соціальних теорій
Інституту інноваційних технологій
Одеського Національного університету імені І.І. Мечникова

Піщевська Е.В.,
кандидат історичних наук,
доцент кафедри соціальних теорій
Інституту інноваційних технологій
Одеського Національного університету імені І.І. Мечникова

ТЕРОРИЗМ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ: НОВІ ТЕНДЕНЦІЇ

Анотація. У статті аналізуються особливості терористичної діяльності, що виникають у зв'язку з появою нових інформаційних технологій. Розглядається, як технології інформаційного суспільства відбиваються на діяльності терористичних організацій. Досліджуються специфіка інформаційного тероризму й шляхи боротьби з ним.

Ключові слова: інформаційне суспільство, тероризм, інформаційно-комунікаційні технології, інформаційний тероризм, міжнародний тероризм.

Інформаційно-комунікаційні технології (ІКТ) давно визнані ефективним інструментом безпеки і стабільності, зміцнення демократії, соціальної згуртованості громадян, належного управління і верховенства права на національному, регіональному і міжнародному рівнях. ІКТ також використовуються для сприяння економічному розвитку суспільства, підвищенню ефективності соціальної політики, розвитку політичної культури громадян. Інформаційні технології забезпечують стабільне функціонування глобальної інформаційної інфраструктури, основу якої складає Інтернет, його успішне використання в бізнесі, освіті і науці, в державному управлінні, життєдіяльності громадянського суспільства.

Проте, не можна не враховувати і негативний момент розвитку ІКТ – можливість їх використання для порушення міжнародного світу і безпеки, підготовки і здійснення злочинів, терористичних актів, поширення терористичної ідеології і практики вирішення суперечностей суспільного розвитку.

Актуальність статті обумовлена тим, що істотна залежність сучасної цивілізації від інформаційної складової зробила її більш уразливою. Швидка дія і широке поширення інформаційних мереж набагато збільшила потужність саме інформаційної зброї. Інтернет породив таке нове явище як кіберзлочинність, що, без сумніву, впливає на політику. Додатково впливає на ситуацію і прийнята сьогодні модель суспільства як принципово відкритого, що передбачає значно більший обсяг всіляких інформаційних потоків, ніж у так званому закритому суспільстві.

Для України актуальність даної проблеми полягає в тому, що, інтегруючись в європейський процес, вона не може бути осторонь проблем сучасних міждержавних відносин. Тероризм – одна з них, отже, своєрідним каталізатором розвитку цієї проблеми в Україні може стати її відкрита зовнішньополітична діяльність [1].

Метою статі є аналіз особливостей терористичної діяльності, що виникають у зв'язку з появою нових інформаційних технологій. Для досягнення даної мети необхідно вирішити такі дослідницькі завдання: розглянути, як технології інформаційного суспільства відбиваються на діяльності терористичних організацій; дослідити специфіку інформаційного тероризму і засоби боротьби з ним.

Як випливає з визначення тероризму, даного в Законі України «Про боротьбу з тероризмом», «Тероризм – суспільно небезпечна діяльність, що полягає в свідомому, цілеспрямованому вживанні насильства шляхом захвату заручників, підпалів, вбивств, залякування населення і органів влади або здійснення інших посягань на життя або здоров'я ні в чому не повинних людей або загрози здійснення злочинних дій з метою досягнення злочинних цілей» [2].

Як відомо, у минулому тероризм був долею груп, що володіють чіткою організаційною і командною структурою, а також конкретним набором політичних, соціальних і економічних цілей і цінностей. Класичні приклади подібних груп – леворадикальні Японська Червона армія і італійські Червоні бригади, а також етнонаціоналістичні організації, наприклад – Ірландська

Республіканська армія, бакскі сепаратисти та ін. Вони орієнтувалися на жорсткі вибіркові акти насильства з метою привернути увагу до себе і своїм ідеям, дотримувалися практики прилюдних заяв, в яких брали відповідальність за здійснені терористичні акції і детально викладали причини, що спонукали їх на ці дії. Жорстка напіввійськова організація, культ дисципліни і єдиноначальності, обов'язкова і регулярна участь у колективних заходах для забезпечення ідейної єдності і згуртованості, прихильність символічно значимому девіантному способу життя і формам поведінки — все це сприяло тому, що лідери і навіть рядові члени терористичних груп, як правило, були поіменно відомі правоохоронним органам і знаходилися під пильним і систематичним наглядом.

Сьогодні разом із звичними типами терористичних угрупувань діють організації нового типа, із значно менш вираженою націоналістичною або ідеологічною ідентичністю.

Таким чином, з одного боку, традиційний тип професійного терориста, ідеологічно мотивованого, такого, що діє відповідно до конкретної політичної програми, оснащеного вибухівкою або вогнепальною зброєю і підтримуваного державами-спонсорами, не зник остаточно. Але, з іншого боку, безумовно, він багато в чому вже витісняється, заміщається тероризмом нового типа, який здатний вести мережеву війну, має інші мотиви, інших акторів і спонсорів, який здатний самоорганізуватися і в набагато більшій мірі спиратися на «непрофесіоналів» Все це робить накопичений аналітичний і практичний дослід боротьби з тероризмом значною мірою застарілим, актуалізуючи потребу у виробленні нових форм і освоєнні нових методів вирішення даного завдання [3].

Тероризм нового типа отримав назву «тероризм в прямому ефірі» або «інформаційний тероризм». Його мета — не лише знищення представників політичної еліти, але і дезорганізація і залякування всього суспільства. Інформаційний тероризм — це форма негативного впливу на особу, суспільства і державу всіма видами інформації. Його мета — послаблення конституційного устрою [4].

Поява електронних мереж створила якісно нові умови і для пропаганди терористами своїх ідей, для ведення ними відкритої полеміки з офіційними державними структурами, дискредитації і дезавуювання заяв офіційних властей. Деякі дослідники підкреслюють нові тенденції в діяльності терористичних організацій, що використовують інформаційно-комунікаційні технології. Все частіше інформаційний тероризм спрямований на пересічних громадян, а не на відповідні, як було раніше, керівні системи [5]. І через те пересічні громадяни виражають свою незадоволеність владою, не здатною їх захистити від проявів тероризму.

Не слід забувати і ту обставину, що з комп'ютеризацією адміністративно-управлінських процесів терористи дістали можливість використовувати в своїх цілях відносно дешеві і доступні методи інформаційно-комп'ютерних диверсій. Поки під удар потрапляють найбільш розвинені країни, в яких широко відкриті електронні системи. Перш за все, це відноситься до США і Канади.

Не випадково фахівці вважають, що в світі високих технологій вже зараз можливі неординарні терористичні акти. Наприклад, опанувавши комп'ютер, який керує літаком, можна диктувати свою волю екіпажу і наземним службам, навіть не здійснюючи озброєного захвату. Відомі випадки, коли злочинці проникали в локальні мережі госпіталів і добиралися до системи життєзабезпечення хворих. Зміна програми може привести до загибелі хворого.

Проблема тероризму є міжнародною, оскільки з нею стикаються багато зарубіжних країн. Терористичні акти в США, Іспанії, Японії, Росії, Англії, Лівані, Іраку, Палестині та інших країнах порушили життя мирних громадян. Такого роду залякування терористів стало способом управління суспільством. Саме у цих цілях міжнародний тероризм прагне до цинічної і широкої демонстрації своїх жорстких атак через засоби масової інформації. За наявними даними, в даний час в 70 країнах налічується близько тисячі груп і організацій, що використовують в своїй діяльності методи терору [6].

Серед дослідників проблем тероризму немає одностайності відносно трактування його сутності, зокрема, міжнародного тероризму. Так, одні дослідники роблять акцент на засобах, способах діяння — засуджують злочинні і антигуманні. Для інших — головною виявляється мотивація, спонукальні причини протизаконного діяння. У першому випадку злочин кваліфікується по формальних ознаках, в другому — по соціальних (тобто, з метою власного збагачення, зміни режиму, залякування опонентів тощо) [7]. Як вважає Ф. Ільясов, «Тероризм, в найзагальнішому сенсі, можна визначити як різні форми «несподіваного» прояву агресії, жертвами якої стають конкретні особи або випадкові скупчення людей, а «інструментом» досягнення мети є формування почуття страху і пригніченості у певних груп людей або у всього населення країни в цілому. Якщо говорити конкретніше, то тероризм — це вбивство, залякування мирного населення, чинення психологічного тиску з метою досягнення економічних і соціальних цілей» [8].

Науково-технічний прогрес розширює можливості міжнародного тероризму щодо провокації у ядерних, екологічних та інформаційних сферах з метою глобальних катастроф. Тому виключно велику небезпеку в сучасних умовах представляє технологічний тероризм, що включає й інформаційний тероризм (а в цілому до технологічного тероризму можна віднести і кібертероризм, і біотероризм, і «ядерний тероризм», і хімічну зброю тощо).

Аналіз наукової літератури, присвяченої інформаційному тероризму, показує, що обговорення проблем протидії військово-політичній загрозі, що виявляється у використанні інформаційно-комунікаційних технологій для досягнення політичних цілей, в даний час має пріоритетне значення. Ймовірно, це можна пояснити тим, що, з одного боку, питання протидії погрозам кіберзлочинності, зокрема кібертероризм, вже досить широко обговорюються на різних міжнародних форумах, а з іншої – інформаційно-комунікаційні технології поступово трансформуються в принципово новий і досить потужний засіб руйнівної дії. Воно може бути спрямоване на об'єкти виробничої і економічної сфер, соціальної інфраструктури, державного управління. Це перетворює дані технології на засіб боротьби, здатний сприяти вирішенню завдань міждержавного протиборства на тактичному, оперативному і стратегічному рівнях.

У цій якості інформаційно-комунікаційні технології набувають властивостей зброї, які зростатимуть через подальше вдосконалення ІКТ, розширення їх повсюдного використання, розвитку інформаційної інфраструктури суспільства і держави, інформатизації озброєння і військової техніки [9].

Таким чином, для продовження інтенсивного розвитку інформаційного суспільства необхідно забезпечити ефективну протидію погрозам використання сучасних інформаційних технологій. І хоча добитися рішучого перелому в протидії загрозам інформаційного тероризму поки що не удалося, певні позитивні тенденції в цій галузі все ж є.

Не секрет, що сучасні інформаційні технології інтенсивно використовуються для підготовки, планування і здійснення терористичних актів, вербування нових членів терористичних організацій, пропаганди екстремістської, у тому числі, терористичної ідеології. Так, останнім часом інформаційний простір все активніше використовується терористами для координації своєї діяльності, організації зв'язку і залучення фінансування. Усвідомлюючи потенціал, яким володіють нові інформаційні технології, ряд міжнародних терористичних організацій останнім часом намагається встановлювати зв'язки з глобальними мережевими співтовариствами хакерів. Терористами ведеться робота по можливому їх залученню в майбутньому для планування і проведення терористичних актів. Доведено, що терористи Аль-Каїди координували свою діяльність саме шляхом використання глобальних мереж. Встановлення робочих контактів між терористами і хакерами загрожує різким стрибком в технологічному розвитку терористів, що може привести до того, що терористи придбають здатність проведення масштабних терактів в інформаційній сфері вже найближчими роками [10].

Мішенями терористів стають комп'ютери і створені на їх основі спеціалізовані системи – банківські, біржові, архівні, дослідницькі, управлінські, а також засоби комунікації – від супутників безпосереднього телемовлення і зв'язку до радіотелефонів і пейджерів.

Новою тенденцією в еволюції тероризму став кібертероризм. Його політична мета – створення суспільної напруженості, страху, дестабілізація обстановки, дискредитація офіційної влади. Фактичною метою його атак виступають комп'ютерні системи управління критичною інфраструктурою, тобто транспортом, атомними електростанціями, водопостачанням і енергетикою. Кібертероризм – це, перш за все, різновид політичного тероризму, завдання якого завжди зводиться до спроби змінити суспільство за допомогою сили.

На думку І. Додіна, під кібертероризмом доцільно розуміти дії окремих осіб або їх груп з дезорганізації роботи автоматизованих інформаційних систем і мереж зв'язку, що створюють небезпеку і можливу загибель людей, спричинення значного майнового збитку або інші суспільно небезпечні наслідки.

До кібертероризму можна віднести також деструктивні дії щодо інформаційних систем, що створюють умови для здійснення актів терроризму [11].

Кібертероризм за допомогою інформаційної зброї може обирати об'єктом своїх актів державні інформаційні ресурси і конфіденційну інформацію. Використання інформаційної зброї, що базується на передових інформаційних і телекомунікаційних технологія з метою завоювання світового панування не лише власне для терористичних організацій, але і для окремих держав і їх коаліцій, що не гребують тероризмом будь-якого вигляду для досягнення своїх політичних амбіцій.

Гостроту проблеми підтверджує і реагування на неї міжнародного співтовариства. Виробленням механізмів вирішення питань кіберзлочинності займаються такі організації, як, наприклад, Форум по управлінню Інтернетом, утворений за підсумками Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства, Міжнародний союз

електрозв'язку, ряд недержавних організацій, експертне співтовариство.

У грудні 1997 р. на зустрічі міністрів внутрішніх справ і юстиції держав «вісімки» в США був підписаний документ «Принципи і план дій боротьби з високотехнологічними злочинами». У травні 2002 р. на зустрічі її представників в Парижі була досягнута домовленість про прийняття країнами «вісімки» аналогічних законів по боротьбі з кіберзлочинністю на національному рівні. У листопаді 2001 р. на конференції в Будапешті представниками 30 країн (у тому числі 26 держав – членів Ради Європи, а також США, Канади, Японії і ЮАР) була підписана Конвенція щодо кіберзлочинності. Відповідно, був створений спеціальний міждержавний орган, що працює в цілодобовому режимі (тобто в режимі інтернет-часу) і має повноваження знищення матеріалів незалежно від фізичного місцезнаходження інтернет-ресурсу. Узгоджувалися національні законодавства, режим розшукових заходів, також передбачалася розробка системи покарання злочинців. Фактично, малося на увазі створення міжнародної кіберполіції з найширшими правами.

Специфіка інформаційного тероризму не у фізичному знищенні людей, ліквідації матеріальних цінностей, руйнуванні життєво важливих об'єктів, а в порушенні роботи інформаційно-комунікативних мереж. Так, за інформацією голови Кіберкомандування США генерала Кіта Александера, мережі міністерства оборони США витримують шість мільйонів хакерських атак за добу. У числі основних джерел мережевої загрози генерал назвав терористів, злочинні угрупування і окремих хакерів. При цьому К. Александер уклав, що інтереси країни знаходяться в небезпеці унаслідок наявності «значних вразливостей» і погроз. Генерал як приклад назвав хакерські DDoS-атаки на урядові ресурси Естонії і Грузії в 2007 і 2008 року. Він також повідомив, що з'явилися і нові погрози безпеці. Так, зараз безпеку Пентагону забезпечують понад 7 мільйонів систем [12].

М. Велічко виділяє такі відмінні риси інформаційного тероризму, як дешевизна і складність виявлення. Система Internet, що зв'язала комп'ютерні мережі всієї планети, змінила правила, що стосуються сучасної зброї. Анонімність, забезпечувана Internetом, дозволяє терористові стати невидимим, як наслідок, практично невразливим і нічим (в першу чергу, життям) не ризикуючи при проведенні злочинної акції [13].

Фахівці вважають, що в світі високих технологій вже зараз можливі неординарні терористичні акти. Так, в 1998 р. в результаті дій кібертерористів в США був убитий особливо важливий свідок, що знаходився в одній з клінік країни під охороною ФБР. Хакер-вбивця, діставши через Інтернет несанкціонований доступ до локальної мережі клініки і зламавши систему захисту інформації, виробив переналагодження кардіостимуляторів хворого, внаслідок чого той загинув [14].

Викладене дозволяє зробити висновок про необхідність вдосконалення інформаційної політики України. Використовуючи досвід західних країн, слід не лише враховувати негативні інформаційні впливи і дії (що, безумовно, поважно), але, в першу чергу, розробити стратегію і тактику інформаційної війни, бо, як говориться, готовлячись до злагоди, не слід запам'ятати і про війну.

Література:

1. Руденко М. М. Інформаційний чинник політики США і Росії в питанні міжнародного тероризму : автореф. дис. ... канд. політ. наук : спец. 23.00.04 : політичні проблеми міжнародних систем та глобального розвитку / М. М. Руденко. – К., 2004. – С. 15.
2. Про боротьбу з тероризмом : Закон України № 638-IV від 20.03.2003 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/638-15
3. Недбай В. В. Социально-политические последствия развития информационного общества: дис. ... канд. полит. Наук : спец. 23.00.02 – политические институты и процессы / В. В. Недбай. – О., 2004. – С. 71-72.
4. Назаренко С. І. ЗМІ – неупереджений свідок чи мимовільний учасник терористичної діяльності / С. І. Назаренко // Сучасна українська політика. Політики і політологи про неї. – Вип. 19. – К., 2010. – С. 265, 267.
5. Назаренко С. І. ЗМІ – неупереджений свідок чи мимовільний учасник терористичної діяльності. – С. 265, 267.
6. Набиев В. Государственная политика в области международного сотрудничества по борьбе с терроризмом / В. Набиев // Власть. – 2007. – № 8. – С. 23-30.
7. Назаренко С. І. ЗМІ – неупереджений свідок чи мимовільний учасник терористичної діяльності. – С. 265.
8. Ильясов Ф. Н. Терроризм – от социальных оснований до поведения жертв / Ф. Н. Ильясов // Социологические исследования. – 2007. – № 6. – С. 82.
9. Тезисы выступления директора Института проблем информационной безопасности МГУ имени М.В. Ломоносова В.П. Шерстюка [Електронний ресурс]. – Режим доступу : http://www.iisi.msu.ru/news/news35/
10. Гриняев С. Россия в глобальном информационном обществе: угрозы, риски и возможные пути их нейтрализации [Електронний ресурс] / С. Гриняев. – Режим доступу : http://www.fondiv.ru/articles/3/335/.
11. Додин И. С. Информационно-коммуникационные технологии в системе государственного управления регионом : автореф. дис ... канд. полит. наук : спец. 23.00.02. – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии (по политическим наукам) / И. С. Додин. – Саратов, 2007. – С. 13.
12. Сети Пентагона атакуют шесть миллионов раз в день [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php7news id=67603.
13. Величко М. Ю. Информационная безопасность в деятельности органов внутренних дел: теоретико-правовой аспект : автореф. дис. ... канд. юрид. наук : спец. 12.00.01 – теория и история права и государства; история учений о праве и государстве / М. Ю. Величко. – Казань, 2007. – С. 18.
14. Томчак Е. В. Из истории компьютерного терроризма / Е. В. Томчак // Новая и новейшая история. – 2007. – № 1. – С. 42.

Дунаева Л.Н., Пищевская Э.В. Терроризм в информационном обществе: новые тенденции. – Статья.

Аннотация. В статье анализируются особенности террористической деятельности, которые возникают в связи с появлением новых информационных технологий. Рассматривается, как технологии информационного общества отражаются на деятельности террористических организаций. Исследуется специфика информационного терроризма и пути борьбы с ним.

Ключевые слова: информационное общество, терроризм, информационно-коммуникационные технологии, информационный терроризм, международный терроризм.

Dunayeva L.N., Pishchevskaya E.V. Terrorism in information-oriented society: new trends. – Article.

Summary. The paper analyzes the features of terrorist activity, arising from the emergence of new information technologies. It considers, how the technologies of information-oriented society affect the activities of terroristic organizations. The specificity of information terrorism and ways of struggle against it are explored.

Key words: information(-oriented) society, terrorism, information and communication technologies, information terrorism, international terrorism.